

**Amendments to the Claims:**

This listing of claims will replace all prior versions, and listings of claims in the application:

**Listing of Claims:**

1-16. (Canceled)

17. (New) An information security policy evaluation system comprising:  
a first information processing apparatus located at a first site;  
a second information processing apparatus located at a second site;  
a third information processing apparatus located at a third site; and  
a fourth information processing apparatus located at a fourth site,  
the first to fourth information processing apparatuses in data communication with  
each other,  
wherein the second information processing apparatus having a treated threat data  
storage section for storing treated threat data, the treated threat data being data indicating a threat  
which can be countered by an information security policy operating at the second site,  
the third information processing apparatus having a threat data storage section for  
storing threat data which is data indicating a previous occurrence of a threat, and a loss amount  
data storage section for storing loss amount data, the loss amount data being data which  
indicates, for each piece of the threat data, a magnitude of a loss occurring in a case where  
damage is suffered due to a threat,  
the second information processing apparatus having a treated threat data  
transmission section for transmitting the treated threat data to the first information processing  
apparatus,  
the third information processing apparatus having a threat data transmission  
section for attaching the loss amount data to the threat data and transmitting the threat data to the  
first information processing apparatus,

22                   the first information processing apparatus having a treated threat data reception  
23 section for receiving the treated threat data and a threat data reception section for receiving the  
24 loss amount data as well as the threat data,

25                   the first information processing apparatus having a correspondence data storage  
26 section for storing correspondence data which is data indicating correspondence between the  
27 threat data and the treated threat data, and a loss amount data storage section for storing the  
28 received loss amount data,

29                   the first information processing apparatus having an effective treated threat data  
30 extraction section for extracting a piece of treated threat data to which there is a piece of threat  
31 data corresponding in the threat data received by the threat data reception section, out of the  
32 treated threat data received by the treated threat data reception section, based on the  
33 correspondence data, and an evaluation data generation section for generating evaluation data in  
34 which the extracted treated threat data is described,

35                   the fourth information processing apparatus having a compensation amount  
36 storage section for storing a compensation amount of insurance which an organization operating  
37 the second site has taken out and which compensates a loss occurring in a case where damage  
38 due to a threat is suffered,

39                   the first information processing apparatus having an evaluation data transmission  
40 section for transmitting the evaluation data generated by the evaluation data generation section to  
41 the fourth information processing apparatus,

42                   the fourth information processing apparatus having an evaluation data reception  
43 section for receiving the evaluation data,

44                   the fourth information processing apparatus having a compensation amount  
45 setting section for resetting the stored compensation amount to the compensation amount  
46 determined in accordance with the evaluation data received by the evaluation data reception  
47 section.

1                   18.     (New) The information security policy evaluation system according to  
2 claim 17 wherein the loss amount data storing section of the third information processing  
3 apparatus stores a monetary damage amount indicating, for said each piece of the threat data, a  
4 magnitude of a loss occurring in a case where damage is suffered due to a threat.

1                   19.     (New) The information security policy evaluation system according to  
2 claim 17, wherein  
3                   the first information processing apparatus has a loss amount data storage section  
4 for storing loss amount data, the loss amount data being data which indicates, for said each piece  
5 of the threat data, a magnitude of a loss occurring in a case where damage is suffered due to a  
6 threat, and  
7                   the evaluation data generation section has a consideration priority sort section for  
8 generating the evaluation data in which the threat data extracted by the untreated threat data  
9 extraction section is sorted and described in descending order of the loss amount data.

1                   20.     (New) The information security policy evaluation system according to  
2 claim 17, wherein  
3                   the threat data transmission section of the third information processing apparatus  
4 attaches the loss amount data to the threat data and transmits the loss amount data to the first  
5 information processing apparatus,  
6                   the threat data reception section of the first information processing apparatus  
7 receives the loss amount data as well as the threat data, and  
8                   the loss amount data storage section of the first information processing apparatus  
9 stores the received loss amount data.

1                   21.     (New) The information security policy evaluation system according to  
2 claim 17 wherein the third information processing apparatus has a threat data update section for  
3 updating the threat data and the threat data transmission section transmits the updated threat data  
4 to the first information processing apparatus in a case where the threat data has been updated by  
5 the threat data update section.

1                   22.     (New) An information security policy evaluation system comprising:  
2 a first information processing apparatus located at a first site;  
3 a second information processing apparatus located at a second site; and  
4 a third information processing apparatus located at a third site,  
5 a fourth information processing apparatus located at a fourth site,  
6 the first to fourth information processing apparatuses in data communication with  
7 each other, wherein:

8                   the second information processing apparatus has a treated threat data  
9 storage section for storing treated threat data, the treated threat data being data indicating  
10 a threat which an information security policy operated on the second site can counter,

11                  the third information processing apparatus has a threat data storage section  
12 for storing threat data which is data indicating a threat having occurred in a past, and a  
13 loss amount data storage section for storing loss amount data, the loss amount data being  
14 data which indicates, for each piece of the threat data, a magnitude of a loss occurring in  
15 a case where damage is suffered due to a threat,

16                  the second information processing apparatus has a treated threat data  
17 transmission section for transmitting the treated threat data to the first information  
18 processing apparatus,

19                  the third information processing apparatus has a threat data transmission  
20 section for attaching the loss amount data to the threat data and transmitting the threat  
21 data to the first information processing apparatus,

22                   the first information processing apparatus has a treated threat data  
23           reception section for receiving the treated threat data and a threat data reception section  
24           for receiving the loss amount data as well as the threat data,

25                   the first information processing apparatus has a correspondence data  
26           storage section for storing correspondence data which is data indicating correspondence  
27           between the threat data and the treated threat data, and a loss amount data storage section  
28           for storing the received loss amount data,

29                   the first information processing apparatus has an untreated threat data  
30           extraction section for extracting a piece of threat data to which there is no piece of treated  
31           threat data corresponding in the treated threat data received by the treated threat data  
32           reception section, out of the threat data received by the threat data reception section,  
33           based on the correspondence data, and an evaluation data generation section for  
34           generating evaluation data in which the extracted threat data is described,

35                   the fourth information processing apparatus has a compensation amount  
36           storage section for storing a compensation amount of insurance which an organization  
37           operating the second site has taken out and which compensates a loss occurring in a case  
38           where damage due to a threat is suffered,

39                   the first information processing apparatus has an evaluation data  
40           transmission section for transmitting the evaluation data generated by the evaluation data  
41           generation section to the fourth information processing apparatus,

42                   the fourth information processing apparatus has an evaluation data  
43           reception section for receiving the evaluation data, and

44                   the fourth information processing apparatus has a compensation amount  
45           setting section for resetting the stored compensation amount to the compensation amount  
46           determined in accordance with the evaluation data received by the evaluation data  
47           reception section.

1                   23.     (New) The information security policy evaluation system according to  
2 claim 22 wherein the loss amount data storing section of the third information processing  
3 apparatus stores a monetary damage amount indicating, for said each piece of the threat data, a  
4 magnitude of a loss occurring in a case where damage is suffered due to a threat.

1                   24.     (New) The information security policy evaluation system according to  
2 claim 22 wherein the third information processing apparatus has a threat data update section for  
3 updating the threat data and, the threat data transmission section transmits the updated threat data  
4 to the first information processing apparatus in a case where the threat data has been updated by  
5 the threat data update section.

1                   25.     (New) An information security policy evaluation system comprising:  
2                   a first information processing apparatus located at a first site;  
3                   a second information processing apparatus located at a second site; and  
4                   a third information processing apparatus located at a third site,  
5                   the first to third information processing apparatuses being capable of  
6 communicating with each other,  
7                   wherein the second information processing apparatus has a policy data storage  
8 section for storing policy data which is data indicating an information about a security policy  
9 operated on the second site,  
10                  wherein the third information processing apparatus has a threat data storage  
11 section for storing threat data which is data indicating a threat having occurred in a past,  
12                  wherein the second information processing apparatus has a policy data  
13 transmission section for transmitting the policy data to the first information processing apparatus,  
14                  wherein the third information processing apparatus has a threat data transmission  
15 section for transmitting the threat data to the first information processing apparatus,  
16                  wherein the first information processing apparatus has a policy data reception  
17 section for receiving the policy data and a threat data reception section for receiving the threat  
18 data,

19                wherein the first information processing apparatus has a correspondence data  
20 storage section for storing correspondence data which is data indicating correspondence between  
21 the threat data and policy data indicating an effective information security policy against a threat  
22 indicated by the threat data, and

23                wherein the first information processing apparatus has an effective policy data  
24 extraction section for extracting a piece of policy data to which there is a piece of threat data  
25 corresponding in the threat data received by the threat data reception section, out of the policy  
26 data received by the policy data reception section, based on the correspondence data, and an  
27 evaluation data generation section for generating evaluation data in which the extracted policy  
28 data is described.

1                26.     (New) An information security policy evaluation system comprising:  
2                a first information processing apparatus located on a first site;  
3                a second information processing apparatus located on a second site; and  
4                a third information processing apparatus located on a third site,  
5                the first to third information processing apparatuses being capable of  
6 communicating with each other,

7                wherein the second information processing apparatus has a policy data storage  
8 section for storing policy data which is data indicating an information about a security policy  
9 operated on the second site,

10               the third information processing apparatus has a threat data storage section for  
11 storing threat data which is data indicating a threat having occurred in a past,

12               the second information processing apparatus has a policy data transmission  
13 section for transmitting the policy data to the first information processing apparatus,

14               the third information processing apparatus has a threat data transmission section  
15 for transmitting the threat data to the first information processing apparatus,

16               the first information processing apparatus has a policy data reception section for  
17 receiving the policy data and a threat data reception section for receiving the threat data,

18                   the first information processing apparatus has a correspondence data storage  
19 section for storing correspondence data which is data indicating correspondence between the  
20 threat data and policy data indicating an effective information security policy against a threat  
21 indicated by the threat data, and

22                   the first information processing apparatus has an untreated threat data extraction  
23 section for extracting a piece of threat data to which there is no piece of policy data  
24 corresponding in the policy data received by the policy data reception section, out of the threat  
25 data received by the threat data reception section, based on the correspondence data, and an  
26 evaluation data generation section for generating evaluation data in which the extracted threat  
27 data is described.

1                   27.     (New) A method of controlling an information security policy evaluation  
2 system having a first information processing apparatus located on a first site, a second  
3 information processing apparatus located on a second site, a third information processing  
4 apparatus located on a third site, a fourth information processing apparatus located on a fourth  
5 site, the first to fourth information processing apparatuses being capable of communicating with  
6 each other, the method comprising:

7                   the second information processing apparatus storing treated threat data, the treated  
8 threat data being data indicating a threat which an information security policy operated on the  
9 second site can counter,

10                  the third information processing apparatus storing threat data which is data  
11 indicating a threat having occurred in a past and loss amount data, the loss amount data being  
12 data which indicates, for each piece of the threat data, a magnitude of a loss occurring in a case  
13 where damage is suffered due to a threat,

14                  the second information processing apparatus transmitting the treated threat data to  
15 the first information processing apparatus,

16                  the third information processing apparatus attaching the loss amount data to the  
17 threat data and transmitting the threat data to the first information processing apparatus,



18                   the first information processing apparatus receiving the treated threat data, the  
19 threat data, and the loss amount data as well as the threat data,

20                   the first information processing apparatus storing correspondence data which is  
21 data indicating correspondence between the threat data and the treated threat data, and the  
22 received loss amount data,

23                   the first information processing apparatus extracting a piece of treated threat data  
24 to which there is a piece of threat data corresponding in the received threat data, out of the  
25 received treated threat data based on the correspondence data, and generating evaluation data in  
26 which the extracted treated threat data is described,

27                   the fourth information processing apparatus storing a compensation amount of  
28 insurance which an organization operating the second site has taken out and which compensates  
29 a loss occurring in a case where damage due to a threat is suffered,

30                   the first information processing apparatus transmitting the evaluation data  
31 generated by the evaluation data generation section to the fourth information processing  
32 apparatus,

33                   the fourth information processing apparatus receiving the evaluation data and  
34 resetting the stored compensation amount to the compensation amount determined in accordance  
35 with the evaluation data received by the evaluation data reception section.

1                   28.     (New) A method of controlling an information security policy evaluation  
2 system having a first information processing apparatus located on a first site, a second  
3 information processing apparatus located on a second site, a third information processing  
4 apparatus located on a third site, a fourth information processing apparatus located on a fourth  
5 site, the first to fourth information processing apparatuses being capable of communicating with  
6 each other, the method comprising:

7                   the second information processing apparatus storing treated threat data, the treated  
8 threat data being data indicating a threat which an information security policy operated on the  
9 second site can counter,

10                   the third information processing apparatus storing threat data which is data  
11                   indicating a threat having occurred in a past and loss amount data, the loss amount data being  
12                   data which indicates, for each piece of the threat data, a magnitude of a loss occurring in a case  
13                   where damage is suffered due to a threat,

14                   the second information processing apparatus transmitting the treated threat data to  
15                   the first information processing apparatus,

16                   the third information processing apparatus attaching the loss amount data to the  
17                   threat data and transmitting the threat data to the first information processing apparatus,

18                   the first information processing apparatus receiving the treated threat data and the  
19                   loss amount data as well as the threat data,

20                   the first information processing apparatus storing correspondence data which is  
21                   data indicating correspondence between the threat data and the treated threat data and the  
22                   received loss amount data

23                   the first information processing apparatus extracting a piece of threat data to  
24                   which there is no piece of treated threat data corresponding in the received treated threat data,  
25                   out of the received threat data based on the correspondence data, and generating evaluation data  
26                   in which the extracted threat data is described,

27                   the fourth information processing apparatus storing a compensation amount of  
28                   insurance which an organization operating the second site has taken out and which compensates  
29                   a loss occurring in a case where damage due to a threat is suffered,

30                   the first information processing apparatus transmitting the evaluation data  
31                   generated by the evaluation data generation section to the fourth information processing  
32                   apparatus,

33                   the fourth information processing apparatus receiving the evaluation data and  
34                   resetting the stored compensation amount to the compensation amount determined in accordance  
35                   with the evaluation data received by the evaluation data reception section.